Claims

What is claimed is:

1. A system for group key management comprising:
   a keying material infrastructure comprising:
      a root portion configured to store a root public key;
      a key encryption key portion operatively connected to the root portion configured to store a traffic encryption key encrypted using a symmetric key encryption key, and a public key encryption key; and
      a first client operatively connected the key encryption key portion configured to store the symmetric key encryption key encrypted using a first client symmetric key; and
   a first group member configured to access the traffic encryption key using the first client symmetric key.

2. The system of claim 1, further comprising:
   a second client operatively connected to the key encryption key configured to store the symmetric key encryption encrypted using a second client symmetric key; and
   a second group member configured to access the traffic encryption key using the first client symmetric key.

3. The system of claim 1, wherein the root portion is further configured to store a private root key encrypted using the traffic encryption key.

4. The system of claim 1, wherein the root portion is further configured to store the traffic encryption key encrypted using the root public key.

5. The system of claim 1, wherein the key encryption key portion is further configured to store a key encryption key encrypted using the symmetric key encryption key.

6. The system of claim 1, wherein the key encryption key portion leaf is further configured to store the traffic encryption key encrypted using the key encryption key.

7. The system of claim 1, wherein the traffic encryption key comprises a version number and a revision number.

8. The system of claim 2, wherein data transferred between the first group member and a second group member is encrypted using the traffic encryption key.

9. The system of claim 1, wherein the first client is further configured to store a first client public key.

10. The system of claim 2, further comprising:

a group owner operatively connected to the keying material infrastructure and configured to manage the first group member and the second group member.

11. The system of claim 10, wherein group owner is configured to store the root public key, the traffic encryption key, the symmetric key encryption key, and the first client symmetric key.

12. The system of claim 11, wherein the group owner is configured to issue at least one selected from the group consisting of a join request and a leave request.

13. The system of claim 1, wherein the first group member is configured to issue at least one selected from the group consisting of a join request and a leave request.

14. A method for group key management for a plurality of group members, comprising:

generating a request to perform at least one operation selected from the group consisting of a traffic encryption key change, a join operation, and a leave operation;

determining whether the one of the plurality of group members initiating the request is a group owner;

determining the one of the plurality of group members upon which the operation is being performed;

rekeying a traffic encryption key and at least one client symmetric key, wherein the at least one client symmetric key is in a path from a client portion of a keying material infrastructure to a root portion of the keying material infrastructure;

generating a root private key and an at least one client private key if the at least one operation is the leave operation;

forwarding the traffic encryption key and the at least one client symmetric key to the plurality of group members using symmetric cryptography if the at least one operation is the join operation and the one of the plurality of group members initiating the request is the group owner;

forwarding the traffic encryption key, the at least one client symmetric key, the root private key, and the at least one client private key to all of the remaining plurality of group members using symmetric cryptography, if the at least one operation is the leave operation and the one of the plurality of group members initiating the request is the group owner;

forwarding the traffic encryption key and the at least one client symmetric key to the plurality of group members using symmetric cryptography and asymmetric cryptography if the at least one operation is the join operation and the one of the plurality of group members initiating the request is not the group owner; and

forwarding the traffic encryption key, the at least one client symmetric key, the root private key and the at least one client private key to all of the remaining plurality of group members using at least one selected from group consisting of symmetric cryptography and asymmetric cryptography if the operation is the leave operation and the one of the plurality of group members initiating the request is not the group owner.

15. The system of claim 15, further comprising:

authenticating the request, wherein the authenticating the request comprises determining whether the group member that initiated the request has sufficient privileges to request the at least one operation.

16. The method of claim 15, wherein rekeying the traffic encryption key comprises applying a one-way function to the traffic encryption key.

17. The method of claim 15, wherein the keying material infrastructure comprises:

the root portion configured to store a root public key;

a key encryption key portion operatively connected to the root portion configured to store a traffic encryption key encrypted using a symmetric key encryption key, and a public key encryption key; and

the first client operatively connected the key encryption key portion configured to store the symmetric key encryption key encrypted using a first client symmetric key.

18. A system comprising a plurality of nodes comprising:

a keying material infrastructure comprising:

a root portion configured to store a root public key;

a key encryption key portion operatively connected to the root portion configured to store a traffic encryption key encrypted using a symmetric key encryption key, and a public key encryption key; and

a first client operatively connected the key encryption key portion configured to store the symmetric key encryption key encrypted using a first client symmetric key; and

a first group member configured to access the traffic encryption key using the first client symmetric key,

wherein root portion is stored on one of the plurality of nodes;

wherein key encryption key portion is stored on one of the plurality of nodes;

wherein the first client is stored on one of the plurality of nodes; and

wherein the first group member is stored on one of the plurality of nodes.